

DIN EN 17529

ICS 35.030

Einsprüche bis 2020-08-05

Entwurf**Datenschutz by Design und als Grundeinstellung;
Deutsche und Englische Fassung prEN 17529:2020**

Data protection and privacy by design and by default;
German and English version prEN 17529:2020

Protection de la vie privée dès la conception et par défaut;
Version allemande et anglaise prEN 17529:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-06-05 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 122 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 17529:2020) wurde von WG 5 „Datensicherheit, Datenschutz und Identitätsmanagement“ des Technischen Komitees CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-01-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

<i>Titel de:</i>	Datenschutz by Design und als Grundeinstellung
<i>Titel en:</i>	Data protection and privacy by design and by default
<i>Titel fr:</i>	Protection de la vie privée dès la conception et par défaut

Inhalt

	Seite
Europäisches Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe und Abkürzungen	6
3.1 Begriffe	6
3.2 Abkürzungen	7
4 Allgemeines	7
4.1 Grundlagen für den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	7
4.2 Struktur für die Zerlegung von Produkten und Diensten in anwendbare Kategorien	9
4.2.1 Einleitung	9
4.2.2 Produktschichten	9
4.2.3 Dienstschichten	10
4.3 Eigenerklärung und Zielerreichungsgrade	11
5 Prozess für eine datenschutzbewusste Entwicklung von Produkten und Diensten	12
5.1 Führung und Marktkennntnis	12
5.2 Vorbereitung	12
5.3 Gestaltung	13
5.3.1 Bestimmung der Anforderungen für DPbPP	13
5.3.2 Entwicklung	14
5.3.3 Produktion und Dienstleistung	14
5.3.4 Freigabe von Produkten und Diensten	14
5.4 Leistungsbewertung	14
5.5 Verbesserung	15
6 Grundlegende Anforderungen an die Gestaltung von Produkten und Diensten	15
6.1 Zugang	15
6.1.1 Zugang zu Daten	15
6.1.2 Kopie der Daten	16
6.2 Verantwortlichkeit	16
6.3 Genauigkeit	17
6.4 Entpersonalisierung von Daten	18
6.5 Datenminimierung	19
6.6 Datenübertragbarkeit	20
6.7 Vertraulichkeit	21
6.8 Löschung	23
6.9 Fairness	24
6.9.1 Bestimmung des Benutzeralters	24
6.9.2 Konfigurierbare Altersgrenze für Kinder	24
6.10 Informationssicherheit	25
6.10.1 Unbefugte oder unrechtmäßige Verarbeitung	25
6.10.2 Datenverlust	28
6.10.3 Ziele des Informationsschutzes	29
6.10.4 Wiederherstellung	30
6.11 Rechtmäßigkeit	30

6.11.1	Datenoffenlegung.....	30
6.11.2	Einwilligung.....	31
6.12	Widerspruch gegen die Verarbeitung.....	31
6.13	Automatisierte Entscheidungsfindung.....	32
6.14	Einschränkung der Verarbeitung.....	32
6.15	Speicherbegrenzung.....	34
6.16	Transparenz.....	34
6.16.1	Informationen.....	34
6.16.2	Verzeichnis von Verarbeitungstätigkeiten	37
7	Anforderungen an die Eigenerklärung datenschutzbewusster Gestaltung.....	38
7.1	Prozessanforderungen.....	38
7.1.1	Vorbereitung basierend auf den Anforderungen der Produkt- und Dienstsicht.....	38
7.1.2	Vorbereitung zusätzlich basierend auf der Durchführung einer DSFA.....	38
7.1.3	Bestimmung des Zielerreichungsgrads.....	39
7.2	Aussage zur Eigenerklärung.....	40
Anhang A (informativ) Zuordnung der Anwendbarkeit zwischen den Anforderungen und Schichten von Abschnitt 6		41
Anhang B (informativ) Ansatz für eine Definition		53
Anhang C (informativ) Leitfaden in Bezug auf EN ISO 9001		55
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den Anforderungen der abzudeckenden Verordnung EU 2016/679 an den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen		60
Literaturhinweise.....		62

Europäisches Vorwort

Dieses Dokument (prEN 17529:2020) wurde von WG 5 „Datensicherheit, Datenschutz und Identitätsmanagement“ des Technischen Komitees CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission und die Europäische Freihandelsassoziation CEN und CENELEC erteilt haben. Dieses Projekt wird als Teil des Arbeitsprogramms des Technischen Komitees CEN/CLC/JTC 13 in Erfüllung des Normungsauftrages M/530 entwickelt.

Zum Zusammenhang mit EU-Richtlinien siehe informativen Anhang ZA, der Bestandteil dieses Dokuments ist.

Einleitung

0.1 Allgemeines

Dieses Dokument stellt den Entwicklern von Komponenten und Teilsystemen einen frühzeitig formalisierten Prozess zur Identifizierung von Datenschutzgegenständen und -anforderungen sowie die notwendige Anleitung für die damit verbundene Abschätzung bereit. Darüber hinaus bietet es Unterstützung für das Verständnis der kaskadierten Haftung und Verpflichtung von Herstellern und Dienstbringern (Verweisung auf DSGVO und ggf. Verweisung auf Artikel 23 sowie auf die für staatliche Anwendungen geltenden Regeln).

Die Datenschutz-Grundverordnung beauftragt in Art. 25 die für die Datenverarbeitung Verantwortlichen und implizit die Hersteller mit der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Ziel dieses Dokuments ist es, Hersteller und/oder Dienstbringer dazu zu verpflichten, Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (DPbDD, en: Data protection and Privacy by Design and by Default) frühzeitig in der Entwicklung ihrer Produkte und Dienste umzusetzen, d. h. vor (oder unabhängig von) einer bestimmten Anwendung oder Integration, um sicherzustellen, dass sie im Hinblick auf die zu erwartenden Märkte möglichst datenschutzfähig sind.

Das Qualitätsmanagementsystem nach EN ISO 9001 bildet den Rahmen für den Prozess zur Bereitstellung von Produkten und Diensten, die den Datenschutz und den Schutz der Privatsphäre von Anfang an berücksichtigen. Falls erforderlich, werden Verbesserungen an EN ISO 9001 vorgenommen. Zusätzlich und soweit in dieser vorläufigen generischen Phase für das Produkt oder den Dienst anwendbar, wurden spezifische Maßnahmenziele und Anforderungen aus der Datenschutz-Grundverordnung abgeleitet, die der jeweilige Lieferant oder Dienstbringer zu erfüllen hat. Schließlich wird ein Eigenerklärungsmechanismus definiert, der, wenn möglich, in Erwartung der Vielfalt der vorgesehenen Anwendungsfälle für entsprechend gestaltete Produkte und Dienste anzuwenden ist, um den für die Datenverarbeitung Verantwortlichen, den betroffenen Personen und der Gesellschaft eine Orientierung zu geben.

Für einige Zwecke der Verarbeitung und für einige Kategorien personenbezogener Daten muss eine Datenschutz-Folgenabschätzung (DSFA) nach EN ISO/IEC 29134 durchgeführt werden, und zusätzlich zu den in diesem Dokument aufgeführten Anforderungen muss auch der aus der DSFA resultierende Behandlungsplan erfüllt werden.

Dieses Dokument ist für die Verwendung durch Hersteller, Lieferanten, Hard- und Softwareentwickler, Systemintegratoren, die Produkte und Dienste für die Verwendung als für die Datenverarbeitung Verantwortliche bereitstellen, sowie für die Verwendung durch Verantwortliche bei der Auswahl von Produkten und Diensten für die Datenverarbeitung bestimmt.

0.2 Kompatibilität mit anderen Managementsystemnormen

Dieses Dokument wendet das von CEN/CENELEC und ISO entwickelte Rahmenwerk an, um die Angleichung zwischen ihren Managementsystemnormen zu verbessern.

Dieses Dokument ermöglicht es einer Organisation, ihre Entwicklungsüberlegungen zum Datenschutz an die Anforderungen anderer Managementsystemnormen anzugleichen oder sie entsprechend zu integrieren.

1 Anwendungsbereich

Dieses Dokument stellt Anforderungen an Hersteller und/oder Dienstleister, Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (DPbDD, en: Data protection and Privacy by Design and by Default) frühzeitig in der Entwicklung ihrer Produkte und Dienste umzusetzen, d. h. vor (oder unabhängig von) einer bestimmten Anwendungsintegration, um sicherzustellen, dass sie möglichst datenschutzfähig sind. Das Dokument wird für alle Wirtschaftszweige, einschließlich der Sicherheitsindustrie, gelten.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN ISO/IEC 29134, *Informationstechnik — Sicherheitsverfahren — Datenschutz-Folgenabschätzung — Leitfaden* (ISO/IEC 29134)

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

— ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

— IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1.1

Datenschutz by Design

technische und organisatorische Maßnahmen zur Umsetzung der Datenschutzgrundsätze

Anmerkung 1 zum Begriff: Die Maßnahmen müssen in wirksamer Weise durchgeführt werden, um den erforderlichen Schutz in die Verarbeitung zu integrieren.

3.1.2

Datenschutz als Grundeinstellung

technische und organisatorische Maßnahmen, um sicherzustellen, dass nur personenbezogene Daten verarbeitet werden, die für jeden spezifischen Zweck der Verarbeitung notwendig sind

Anmerkung 1 zum Begriff: Solche Maßnahmen sollten mindestens die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, die Speicherfrist und ihre Zugänglichkeit umfassen.

3.1.3

Datenschutz-Folgenabschätzung

DSFA

Gesamtprozess aus Identifizieren, Analysieren, Bewerten, Beraten, Kommunizieren und Planen der Behandlung von möglichen Datenschutzfolgen unter Bezug auf die Verarbeitung personenbezogener Daten, eingebettet in das unternehmensweite Rahmenwerk zum Risikomanagement

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 29134:2017, 3.7.

3.1.4

besondere Kategorien personenbezogener Daten

Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

[QUELLE: DSGVO Artikel 9, Abschnitt 1]

3.2 Abkürzungen

DPbDD	Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (en: Data protection and Privacy by Design and by Default)
DSFA	Datenschutz-Folgenabschätzung
DSGVO	EU-Datenschutz-Grundverordnung
GSMA	Global System for Mobile Communications Association
ISACA	Information Systems Audit and Control Association
LoA	Zielerreichungsgrad (en: Level of Achievement)

4 Allgemeines

4.1 Grundlagen für den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Neben den weit gefassten Erwartungen an den Schutz personenbezogener Daten bei Datenverarbeitungsverfahren beziehen sich Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen auf die Fähigkeit der vorgesehenen technischen Systeme und Komponenten, diesen Schutz unterstützen zu können. Dennoch sind die Hersteller nach DSGVO nicht dazu verpflichtet. Es sind daher andere Instrumente erforderlich, um sie in einem Prozess zu begleiten, durch den ihre Produkte oder Dienste so ausgelegt werden, dass sie den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen für ein Maximum an Anwendungsfällen entsprechend dem erwarteten Markt erfüllen. Eine zugrunde liegende Reihe von Anforderungen, die mit dem Qualitätsprozess des Unternehmens konsistent sind, werden im Folgenden detailliert beschrieben. Erwartete Vorteile sind für die Endbenutzer (Kunden/Datenverantwortliche) die einfache Umsetzung ihrer Datenschutzpflichten und für den Hersteller ein Wettbewerbsvorteil.

Die DSGVO enthält viele gesetzliche Bestimmungen, die von den für die Datenverarbeitung Verantwortlichen und den Auftragsverarbeitern in Betracht gezogen werden können; solche Bestimmungen hängen weitgehend von den unterschiedlichen funktionalen und betrieblichen Bedingungen ab, unter denen das Produkt oder der Dienst voraussichtlich verwendet wird. In diesem Zusammenhang und um die Anbieter von Produkten und Diensten bei ihrer Abschätzung zu unterstützen, wurden die Verpflichtungen der für die Datenverarbeitung Verantwortlichen generisch analysiert, wenn sie explizit oder implizit den Bedarf an funktionalen Fähigkeiten zur Unterstützung der Verpflichtung der für die Datenverarbeitung Verantwortlichen enthalten.

Die folgenden Grundsätze werden als grundlegend für den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen betrachtet:

- 1) DPbDD muss proaktiv und präventiv, nicht reaktiv und korrektiv sein.
- 2) Standardeinstellungen und -konfiguration müssen sicher und datenschutzbewusst sein.
- 3) Datenschutz und Schutz der Privatsphäre müssen in die Gestaltung einbezogen werden.
- 4) DPbDD strebt nach voller Funktionalität im Einklang mit legitimen Interessen und Zielen, ohne Kompromisse.
- 5) DPbDD betrifft den gesamten Datenlebenszyklus.
- 6) DPbDD muss sichtbar und transparent sein und einer unabhängigen Verifizierung unterliegen.
- 7) Die Interessen des Einzelnen sollten im Vordergrund stehen, indem starke Vorgaben und eine angemessene Benachrichtigung angeboten werden, und die Benutzer sollten durch benutzerfreundliche Optionen im Mittelpunkt stehen, auch wenn solche Bestimmungen als weniger datenschutzfreundlich erscheinen.
- 8) Die Maßnahmen für DPbDD müssen wirksam sein.
- 9) Die Maßnahmen für DPbDD müssen so ausgelegt werden, dass sie robust sind und in Übereinstimmung mit dem erhöhten Risiko einer Verletzung der Datenschutzgrundsätze aufgestockt werden können.
- 10) Die Maßnahmen für DPbDD müssen regelmäßig bewertet werden.

Wenn Datenschutz by Design so weit wie möglich verstanden werden soll, darf nicht nur der Zeitpunkt der Lieferung und Bereitstellung berücksichtigt werden. Der gesamte Lebenszyklus sowohl der personenbezogenen Daten als auch des Produkts und/oder des Dienstes muss ebenfalls berücksichtigt werden.

Besonderes Augenmerk sollte auf Instandhaltungsmaßnahmen sowie auf die Rahmenbedingungen gelegt werden, unter denen eine Wiederverwendung von Produkten stattfinden könnte. Darüber hinaus umfasst der Dienst den Vorgang der Verarbeitung als Auftragsverarbeiter im Auftrag der für die Datenverarbeitung Verantwortlichen. Einige Anforderungen dieses Dokuments werden die Aufmerksamkeit auf diese Szenarien lenken.

Wenn der Dienstbringer selbst als für die Datenverarbeitung Verantwortlicher angesehen werden muss, sollten zusätzliche organisatorische und technische Maßnahmen ergriffen und durch ein geeignetes Managementsystem, z. B. EN ISO/IEC 27701, geregelt werden. Diese organisatorischen und technischen Maßnahmen liegen außerhalb des Anwendungsbereichs dieses Dokuments.

Dieses Dokument bietet in 4.2 eine Struktur für die Aufteilung integrierter Produkte und Dienste in Schichten, die verwendet werden dürfen, um sie in Bausteine zu modulieren, die die gleiche Reihe von Anforderungen erfüllen müssen. In 4.3 wird das Konformitätsschema für eine Eigenerklärung angegeben.

In Abschnitt 5 werden die Anforderungen für einen Prozess der datenschutzbewussten Entwicklung von Produkten und Diensten angegeben.

In Abschnitt 6 gibt es grundlegende Anforderungen an die Gestaltung der bereitgestellten Produkte und Dienste. Die Anwendung wird für die jeweiligen in 4.2 definierten Produkt- und Dienstsichten festgelegt, und die Maßnahmenziele nehmen Bezug auf die DSGVO.

Abschnitt 7 enthält einen Leitfaden für den Prozess der Eigenerklärung und die Anforderungen zur Bestimmung des Zielerreichungsgrads.

In Anhang A, Anhang B und Anhang C werden detaillierte Informationen über die Zuordnung der grundlegenden Anforderungen an Produkt- oder Dienstsichten, über die Definition des eingebauten Datenschutzes und über eine Anleitung zur Anwendung von ISO 9001 als Managementsystem bei der Entwicklung gegeben. Zusätzlich enthält der Anhang ZA die Konformitätserklärung für den EU-Normungsauftrag M/530.

4.2 Struktur für die Zerlegung von Produkten und Diensten in anwendbare Kategorien

4.2.1 Einleitung

Da es nicht praktikabel erscheint, Anforderungen direkt für Produkte und Dienste zu erstellen, die sich in der Zusammensetzung, Architektur und Bündelung von Untermodulen stark unterscheiden können, wird in den nächsten beiden Abschnitten eine Reihe von Modulkategorien definiert. Jedes Marktprodukt oder jeder Marktdienst im Rahmen dieses Dokuments muss als eine Kombination einiger dieser Kategorien betrachtet werden, wenn es darum geht, Schichten hinzuzufügen, um ein vollständiges Bild zu erhalten. Daher werden für diese Kategorien die Begriffe „Produktschicht“ und „Dienstschicht“ verwendet.

4.2.2 Produktschichten

Die Modulkategorien, aus denen ein Produkt bestehen kann, sind wie folgt definiert:

- 1) Komponentenschicht – hauptsächlich physikalische Untermodule wie Mikroprozessoren und Mikrocontroller, DRAM-Module, Schnittstellen-Controller, Medienlaufwerke, physikalische Speichermedien, Sensoren, Aktoren oder Stromversorgung. Diese Schicht kann Konnektivitätstreiber und kleine Programme wie z. B. zur Aufrüstung oder dynamischen Verbindung enthalten.
- 2) Geräteschicht – Barebone mit Einbaurahmen, Abschirmung, Display, Tastaturen und Gehäuse. Die Geräteschicht integriert Komponenten aus der Komponentenschicht und fügt Programme für BIOS und Boot-Fähigkeiten hinzu.
- 3) Betriebssystemsicht – Softwareschicht mit Programmen, die sich für die Konfiguration des Geräts, die grundlegende Interaktion mit dem Benutzer, wie Tastatureingabe und -ausgabe über Bildschirm oder Drucker, die Unterstützung der Benutzerauthentifizierung, die Verwaltung des Geräts selbst und seine Interkonnektivität mit Netzwerken und mit Werkzeugen, die lokale Maßnahmen auf dem Gerät unterstützen, eignen.
- 4) Kommunikationsschicht – Konnektivitätskomponenten, die physikalische Verbindungen (drahtgebunden oder drahtlos) zum Zweck der Informationsübertragung emulieren. Diese Schicht ähnelt der Komponentenschicht, unterscheidet sich jedoch hinsichtlich spezifischer Belange, die mit dem Aspekt des von ihr aufgebauten Netzwerks zusammenhängen.
- 5) Speicherschicht – logische Schicht für das Management von Speicherorten auf angeschlossenen physischen Speichermedien über die Komponentenschicht. Dazu gehören lokal oder per Fernzugriff angeschlossene Medien, Raid- oder Cluster-Architekturen, NAS- oder SAN-Konzepte sowie Fileserver und Cloud-Storage.
- 6) Benutzungsschnittstellenschicht – logische Schicht für das Management der Benutzerinteraktion mit einem Gerät oder Dienst, die sich nicht auf der Betriebssystemsicht befindet. Zu dieser Schicht gehören auch Portale und bis zu einem gewissen Grad Content-Management-Systeme.
- 7) Integrierte Systemsicht – diese Schicht gilt, wenn ein Produkt eine Integration von mehr als einem Gerät ist. Sie erfordert ein Kommunikationsmodell zwischen den Geräten mit spezifizierten Protokollen und Übertragungsmanagement. Integrierte Systeme müssen die Fähigkeiten und Standardeinstellungen für eine angemessene Netzwerksicherheit nachweisen.
- 8) Anwendungsschicht – Softwareschicht, die die erwartete Funktionalität eines Geräts oder eines integrierten Systems bereitstellt.

- 9) Geschäftsprozessschicht – logische Schicht über der Anwendungsschicht, die den Informationsaustausch zwischen vielen Geräten, integrierten Systemen oder sogar Organisationen verwaltet.
- 10) Systemmanagementschicht – logische Schicht für das Management der Betriebs- und Informationssicherheit in Bezug auf die Geräte, integrierten Systeme, Anwendungen, Speicher und/oder Kommunikationsflüsse.

4.2.3 Dienstschichten

Die Modulkategorien, aus denen ein Dienst bestehen kann, sind wie folgt definiert:

- 1) Dienstmanagementschicht – menschlich basierter Dienst zur Konfiguration, Betriebssteuerung und Reaktion auf einen Zwischenfall.
- 2) Selbstbedienungsschicht – Anwendungsdienst, der dem Kunden oder Benutzer Werkzeuge zur Konfiguration anderer Produkt- oder Dienstschichten zur Verfügung stellt.
- 3) Integrationsdienstschicht – kundenspezifischer Dienst zur Herstellung der Interoperabilität von Teilsystemen, der üblicherweise innerhalb eines dedizierten Projekts unter einem vom Kunden definierten Managementrahmen organisiert wird.
- 4) Übertragungsdienstschicht – Dienst, der Übertragungsleitungen über organisatorische Grenzen miteinander verbindet.
- 5) Aktualisierungsdienstschicht – Programmcode-Updates, die proaktiv von Menschen, automatisch reaktiv oder nur durch Bereitstellung der Updates zum Download bereitgestellt werden.
- 6) Cloud-Dienstschicht – Dienstbereitstellung von Betriebseinrichtungen entweder auf Infrastruktur- oder auf Anwendungsebene.
- 7) Inhaltsdienstschicht – Dienst, der zusätzliche Daten (z. B.: Nachrichten, Bewertungszahlen, Adressen) zur Verfügung stellt, manchmal mit der Möglichkeit, erhobene personenbezogene Daten zu verbessern.
- 8) Ausgliederte Geschäftsprozessschicht – funktionale Datenverarbeitung entweder kundenspezifisch oder als normalisiertes Angebot an ähnliche Kunden.
- 9) Ausgabedienstschicht – Dienste, die Kundendaten zum Zweck der Produktion von Ausgabemedien (z. B.: Fotokalender oder Marketing-E-Mails) empfangen.
- 10) Wartungsdienstschicht – Dienst, der auf Anforderung von Anwendern und/oder Kunden reagiert, um Produkte und Dienste über die gesamte Lebensdauer nutzbar zu halten, einschließlich Abhol- oder Bringdienste und Gerätetausch.
- 11) SaaS-Schicht – halbautomatische Dienste, die Systeme, Verkehr und Protokolleinträge auswerten, um Anfälligkeiten und Sicherheitsverletzungen zu erkennen, zu verhindern oder darauf zu reagieren.
- 12) Medienwiederherstellungsdienstschicht – Dienst auf kundeneigenen physischen Speichermedien zum Zweck der Wiederherstellung der darin enthaltenen Informationen.
- 13) Medienvernichtungsdienstschicht – physische Vernichtung von Speichermedien auf eine Art und Weise, die eine Wiederherstellung von Daten unmöglich macht, üblicherweise am Ende des Lebenszyklus.
- 14) Systemwiedervermarktungsdienstschicht – Dienst an Produkten durch Reinigung, Rekonstruktion und Neulizenzierung, um dem Produkt ein zweites Leben bei einem anderen Kunden zu ermöglichen.

4.3 Eigenerklärung und Zielerreichungsgrade

Obwohl die Berücksichtigung des Datenschutzes und des Schutzes der Privatsphäre durch Technikgestaltung im Rahmen des Qualitätsmanagementsystems einer Organisation als Voraussetzung für die Bereitstellung von DPbDD angesehen werden könnte, würde es nicht ausreichen, die entsprechenden Prozesse einzuhalten, um datenschutzbewusste Produkte und Dienste zu entwickeln. Es ist auch unabdingbar, dass das Produkt oder der Dienst den spezifischen Anforderungen entspricht, die für jede der Schichten gelten, aus denen das Produkt oder der Dienst aufgebaut ist, um die Grundsätze des Datenschutzes und des Schutzes der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu erfüllen.

In der Praxis wäre es manchmal vernünftig, einen Kompromiss zwischen den Marktbedürfnissen oder den von Kunden geäußerten Anforderungen sowie den Grundsätzen und Anforderungen zu finden. Dies wird das Schutzniveau für die betroffene Person senken, aber nicht zu einem Produkt oder einem Dienst führen, das bzw. der datenschutzunfreundlich ist. Als weiteres Beispiel könnte eine Organisation planen, ein Produkt oder einen Dienst für die Verarbeitung spezieller Datenkategorien unter rechtmäßigen Umständen bereitzustellen, und sie wendet zusätzliche Maßnahmen oder Funktionen an, die aus einer Datenschutz-Folgenabschätzung abgerufen wurden. Ein datenschutzbewusster Zustand wird nicht das erhöhte Maß an Schutz widerspiegeln, das erforderlich ist und durch zusätzliche Anstrengungen nachgewiesen wird.

Um sowohl die Praxis der Kompromisse als auch die Notwendigkeit der Angemessenheit unter besonderen Verarbeitungsbedingungen widerzuspiegeln, wurden in der nachstehenden Tabelle 1 sechs Zielerreichungsgrade definiert.

Tabelle 1 — Definitionen von Zielerreichungsgraden

Zielerreichung	Untergeordnete Zielerreichung	Zielerreichungsgrad	Voraussetzungen
Die Anforderungen werden vollständig erfüllt. Es wurden keine Kompromisse eingegangen. Spezielle Kategorien personenbezogener Daten stehen kurz vor der Verarbeitung, und es wurden dementsprechend zusätzliche Gestaltungsanliegen geäußert.	Spezielle Kategorien für den Schutz personenbezogener Daten und den Schutz der Privatsphäre werden durch Technikgestaltung und datenschutzfreundliche Voreinstellungen berücksichtigt.	A	Eine Datenschutz-Folgenabschätzung wurde durchgeführt und entsprechende Gestaltungsanliegen wurden berücksichtigt.
Die Anforderungen werden vollständig erfüllt. Es wurden keine Kompromisse eingegangen. Der Zweck passt zum Schutzniveau.	Datenschutz und Schutz der Privatsphäre werden durch Technikgestaltung und datenschutzfreundliche Voreinstellungen erwogen.	B	Die Anforderungen werden vollständig erfüllt. Es wurden keine Kompromisse eingegangen. Die vorrangige Berücksichtigung der Interessen der betroffenen Person wird bestätigt.
Bei der Anwendung der Anforderungen wurden Kompromisse eingegangen	Die Technikgestaltung ist datenschutzbewusst.	C	Die Anforderungserfüllungsrate beträgt $95 \% < x < 100 \%$.
	Die Technikgestaltung ist größtenteils datenschutzbewusst.	D	Die Anforderungserfüllungsrate beträgt $80 \% < x < 95 \%$.
	Überlegungen zu einer datenschutzbewussten Technikgestaltung wurden im Allgemeinen angestellt.	E	Die Anforderungserfüllungsrate beträgt $50 \% < x < 80 \%$.
Die Anwendung der Anforderungen ist unzureichend		Z	Die Anforderungserfüllungsrate ist niedriger als 50 %.

Zielerreichungen müssen durch Konformität mit den Anforderungen nachgewiesen werden, die aus der richtigen Reihe von Produkt- und/oder Dienstsichten anwendbar sind. Im Falle einer bestimmten Verarbeitung, die wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt, muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden, deren Ergebnis ebenfalls in die Technikgestaltung einbezogen werden muss. Diese DSFA muss durchgeführt und aufgezeichnet werden. Ein Beispiel für eine DSFA wird durch EN ISO/IEC 29134 bereitgestellt.

Lieferanten und Dienstleister dürfen ihr Produkt oder ihren Dienst durch eine Eigenerklärung zusammen mit der Zielerreichung als datenschutzbewusst kennzeichnen, sofern sie die Konformität mit den Anforderungen entsprechend Abschnitt 7 nachweisen können.

5 Prozess für eine datenschutzbewusste Entwicklung von Produkten und Diensten

5.1 Führung und Marktkennntnis

5.1.1 Die Organisation muss das Verständnis für Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, das für die Entwicklung und Bereitstellung ihrer Produkte und Dienste unabdingbar ist, schaffen und aufrechterhalten.

ANMERKUNG Dies bedeutet, dass der Datenschutz und der Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in der Verpflichtung der Unternehmensleitung zum Ausdruck kommt, die sich in schriftlichen Politiken ausdrückt, und dass die jeweiligen Verantwortlichkeiten und die Rechenschaftspflicht den entsprechenden organisatorischen Rollen zugewiesen werden.

5.1.2 Um eine angemessene Übereinstimmung zwischen der Vielfalt der durch den Zielmarkt implizierten Anwendungsfälle und deren Auswirkungen auf die Aktivierung der DSGVO-Bestimmungen sicherzustellen, muss die Organisation das für den nachstehenden Prozess verantwortliche Personal auswählen, schulen und umfassend über die DSGVO und ihre funktionale Logik informieren, eine umfassende Übersicht über alle Nutzungsbedingungen in Bezug auf die verschiedenen Segmente, die von den Marketingplänen abgedeckt werden.

Diese umfassende funktionale Sichtweise gilt für den gesamten in diesem Abschnitt 5 beschriebenen Prozess, wobei zu berücksichtigen ist, dass die Datenschutzanalyse in Bezug auf die spezifische Beschaffung eines Produkts oder Systems außerhalb des Anwendungsbereichs dieses Dokuments liegt.

5.2 Vorbereitung

5.2.1 Die Organisation muss bestimmen, ob das Geschäftsmodell eine aktive Rolle bei der Verarbeitung personenbezogener Daten vorsieht.

ANMERKUNG Eine aktive Rolle muss in Betracht gezogen werden, wenn die personenbezogenen Daten für Produkte oder Dienste verarbeitet werden, bei denen der Kunde und/oder Benutzer nicht die volle und alleinige Kontrolle über die Erhebung, Speicherung, gemeinsame Nutzung und Löschung dieser personenbezogenen Daten hat.

5.2.2 Um die Auswirkungen von Produkten und Diensten auf die Privatsphäre einer betroffenen Person zu behandeln, muss die Organisation eine geeignete Methodik und die Struktur des Berichts festlegen.

ANMERKUNG EN ISO/IEC 29134 enthält Anleitungen für die Datenschutz-Folgenabschätzung

5.2.3 Die Organisation muss den Entwicklungsabteilungen Zugang zu ausreichenden personellen Ressourcen mit der entsprechenden Kompetenz in rechtlichem und technischem Fachwissen auf dem Gebiet des Datenschutzes gewähren.

Wenn ein Datenschutzbeauftragter für die Organisation ernannt wird, sollte dieser in den Gestaltungsprozess einbezogen werden. Eine andere Option könnte darin bestehen, eine spezielle Rolle als Datenschutzingenieur in der Entwicklungsabteilung zu übernehmen.

5.2.4 Die Organisation muss ihren bestehenden Entwicklungsprozess auf die Eignung zur Erfüllung der Anforderungen dieses Dokuments bewerten und erforderlichenfalls ändern.

5.3 Gestaltung

5.3.1 Bestimmung der Anforderungen für DPbPP

5.3.1.1 Grundlegende Anforderungen an die Gestaltung

5.3.1.1.1 Die für die Produkt- und/oder Dienstgestaltung verantwortliche Person muss das beabsichtigte Marktangebot logisch in die Schichten zerlegen, aus denen es sich zusammensetzt.

ANMERKUNG Die Schichten sind in 4.2 definiert.

5.3.1.1.2 Für jede Schicht, die als Teil des beabsichtigten Marktangebots identifiziert wurde, müssen alle für diese Schicht geltenden grundlegenden Anforderungen aus Abschnitt 6 ermittelt werden.

ANMERKUNG Anhang A, Tabelle A.1 und Tabelle A.2 enthalten Zuordnungstabellen für die anwendbaren grundlegenden Anforderungen an eine bestimmte Produkt- oder Dienstschiicht.

5.3.1.2 Erweiterte Gestaltungsanforderungen bei der Verarbeitung personenbezogener Daten

5.3.1.2.1 Für den Fall, dass die Organisation bestätigt hat, eine aktive Rolle bei der Verarbeitung personenbezogener Daten für das beabsichtigte Marktangebot zu übernehmen, muss die für die Produkt- und/oder Dienstgestaltung verantwortliche Person die Umsetzung geeigneter technischer und organisatorischer Maßnahmen in Betracht ziehen.

ANMERKUNG 1 EN ISO/IEC 27701, Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Schutz der Privatsphäre, enthält entsprechende Anforderungen und einen Leitfaden.

Wenn es einen Datenschutzbeauftragten der Organisation gibt, sollte dieser informiert und konsultiert werden, um die geeigneten Maßnahmen zur Durchführung der Verarbeitung zu bestimmen.

ANMERKUNG 2 Es wird auf DSGVO Artikel 25 verwiesen.

5.3.1.3 Folgenbedingte Gestaltungsanforderungen

5.3.1.3.1 Die für die Produkt- und/oder Dienstgestaltung verantwortliche Person muss bestimmen, ob die erhobenen, verarbeiteten und/oder übermittelten Daten so genannte „besondere Kategorien personenbezogener Daten“ im Sinne von Artikel 9 DSGVO oder personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten enthalten.

ANMERKUNG Es wird auf DSGVO Artikel 9 und Artikel 10 verwiesen.

5.3.1.3.2 Falls die besonderen Kategorien personenbezogener Daten bestätigt werden, muss die für die Produkt- und/oder Dienstgestaltung verantwortliche Person eine Datenschutz-Folgenabschätzung (DSFA) in Übereinstimmung mit den Bestimmungen in 5.2.2 durchführen.

ANMERKUNG Es wird auf DSGVO Artikel 35 verwiesen. Es könnte weitere Fälle geben, in denen ebenfalls eine DSFA durchgeführt werden muss.

5.3.1.3.3 Kommt die DSFA zu dem Schluss, dass zusätzliche Anforderungen an die Gestaltung und die Standardeinstellung des Produkts und/oder des Dienstes gestellt werden müssen, muss die für die Gestaltung des Produkts und/oder des Dienstes verantwortliche Person sicherstellen, dass diese Anforderungen bei der Entwicklung ebenfalls berücksichtigt werden.

5.3.1.4 Spezielle Geschäftsbereiche oder verbraucherbezogene Gestaltungsanforderungen

5.3.1.4.1 Wenn ein Produkt und/oder ein Dienst für bestimmte Kategorien von betroffenen Personen bereitgestellt werden sollen, muss die für die Produkt- und/oder Dienstgestaltung verantwortliche Person bestimmen, ob besondere Erwartungen an die datenschutzbewusste Gestaltung und die Standardkonfiguration bestehen.

5.3.1.4.2 Jede dieser Erwartungen muss entweder durch eine bestehende oder eine neue Anforderung an die Gestaltung und die Standardeinstellung des Produkts und/oder des Dienstes abgedeckt werden. Die für die Gestaltung des Produkts und/oder des Dienstes verantwortliche Person muss sicherstellen, dass diese Anforderungen bei der Entwicklung ebenfalls berücksichtigt werden.

ANMERKUNG In einen bestimmten Geschäftsbereich, einem bestimmten Anwendungsfall oder einer bestimmten Umgebung könnten die Kunden- und/oder Verbrauchererwartungen an eine datenschutzbewusste Technikgestaltung und datenschutzfreundliche Voreinstellungen weitaus detaillierter sein als die rechtlichen Erwartungen aus der DSGVO.

5.3.2 Entwicklung

5.3.2.1 Die für die Entwicklung des Produkts und/oder des Dienstes verantwortliche Person muss sicherstellen, dass alle in 5.3.1 aufrechterhaltenen Gestaltungsanforderungen in der Entwicklungsphase des Produkts oder des Dienstes berücksichtigt werden.

5.3.2.2 Die für die Entwicklung des Produkts und/oder des Dienstes verantwortliche Person muss sicherstellen, dass die größten Anstrengungen unternommen werden, um angemessene Funktionen, Maßnahmen und Kontrollen in dem jeweiligen Produkt und/oder dem Dienst zu implementieren, um die in 5.3.2.1 genannten Anforderungen zu erfüllen.

5.3.2.3 Die für die Entwicklung des Produkts und/oder des Dienstes verantwortliche Person muss für jede konfigurierbare Funktion, die mit dem in Entwicklung befindlichen Produkt und/oder dem Dienst geliefert wird, so weit wie möglich datenschutzbewusste Voreinstellungen festlegen.

ANMERKUNG Als Leitgrundsatz ist die Datenminimierung zu berücksichtigen.

5.3.2.4 Die für die Entwicklung des Produkts und/oder des Dienstes verantwortliche Person muss sicherstellen, dass die Voreinstellungen des Produkts und/oder des Dienstes mit den in 5.3.2.3 definierten Einstellungen übereinstimmen.

5.3.3 Produktion und Dienstleistung

5.3.3.1 Die Organisation muss geeignete Prüfungen durchführen und entsprechende Nachweise dokumentieren, um die Umsetzung der Funktionen, Maßnahmen und Kontrollen aus 5.3.2.2 und der Standardkonfiguration aus 5.3.2.4 zu bestätigen.

5.3.3.2 Für das Produkt und/oder den Dienst muss die Organisation den Zielerreichungsgrad bestimmen.

ANMERKUNG 7.1.3 enthält die Anforderungen für die Bestimmung des Zielerreichungsgrads.

5.3.4 Freigabe von Produkten und Diensten

5.3.4.1 Die Organisation muss dem Kunden schriftliche Informationen in einfacher Sprache als Teil der Produktdokumentation über alle datenschutzbezogenen Funktionen und Einstellungen des freigegebenen Produkts und/oder Dienstes zur Verfügung stellen.

5.4 Leistungsbewertung

5.4.1 Wenn die Organisation einen Jahresbericht über die soziale Verantwortung der Unternehmen vorlegt, muss dieser Bericht auch den Prozentsatz der Produkte und Dienste nach ihrem jeweiligen Zielerreichungsgrad enthalten. Nach dem ersten Jahr der Berichterstattung muss auch die Abweichung gegenüber dem vorangegangenen Bericht oder einem anderen geeigneten Bezugsjahr angegeben werden.

5.5 Verbesserung

5.5.1 Die Organisation muss alle datenschutzbezogenen Rückmeldungen von Kunden, Anwendern und anderen Anspruchsgruppen zu dem freigegebenen Produkt und/oder Dienst beachten.

5.5.2 In regelmäßigen Abständen, spätestens mit Beginn der Gestaltung für die nächste größere Freigabe, müssen die in 5.5.1 erhaltenen Rückmeldungen ausgewertet und spezifische Erwartungen für die neue Freigabe thematisiert werden.

5.5.3 Jede Anforderung, die im Rahmen der aktuellen Entwicklung nicht erfüllt werden konnte, muss aufgezeichnet werden, und sie wird zu einer Anforderung, die von der nachfolgenden Freigabe des Produkts und/oder des Dienstes abhängt.

6 Grundlegende Anforderungen an die Gestaltung von Produkten und Diensten

6.1 Zugang

6.1.1 Zugang zu Daten

6.1.1.1 Maßnahmenziel:

Bereitstellung von Fähigkeiten für die betroffene Person, auf ihre Daten zuzugreifen.

ANMERKUNG Es wird auf DSGVO Artikel 15, Abschnitt 1 verwiesen.

6.1.1.2 Das Rollenmodell des Produkts muss eine Zugriffsrolle für die betroffene Person vorsehen, die einen Lesezugriff auf jeden Datensatz ermöglicht, der mit der spezifischen betroffenen Person verknüpft ist.

Diese Anforderung gilt für die folgenden Produktschichten:

- Benutzungsschnittstellenschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Inhaltsdienstschicht und
- ausgegliederte Geschäftsprozessschicht.

ANMERKUNG Anschließend werden benötigte Zugriffsrechte z. B. für Verzeichnisse oder Datentabellen aufgenommen.

6.1.1.3 Der Dienst muss ein Konto für jede betroffene Person zur Verfügung stellen, um Zugang zu den von ihr erhobenen, verarbeiteten oder gespeicherten persönlichen Datensätzen zu erhalten.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Inhaltsdienstschicht und
- ausgegliederte Geschäftsprozessschicht.

6.1.2 Kopie der Daten

6.1.2.1 Maßnahmenziel:

Bereitstellung von Fähigkeiten zur Bereitstellung einer Kopie der personenbezogenen Daten in einer häufig verwendeten elektronischen Form.

ANMERKUNG Es wird auf DSGVO Artikel 15, Abschnitt 3 verwiesen.

6.1.2.2 Das Produkt und/oder der Dienst müssen eine Exportfähigkeit für Datensätze in einem für Personen lesbaren Format bieten.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Speicherschicht;
- Benutzungsschnittstellenschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Cloud-Dienstschicht;
- Inhaltsdienstschicht und
- ausgegliederte Geschäftsprozessschicht.

ANMERKUNG Dies könnte auch durch die Bereitstellung von Transformationswerkzeugen für ein von Personen nicht lesbares Format erreicht werden.

6.2 Verantwortlichkeit

6.2.1 Maßnahmenziel:

Um alle vernünftigen Belege, die aufgezeichnet wurden, vorzulegen, muss der für die Datenverarbeitung Verantwortliche möglicherweise die Einhaltung nachweisen.

ANMERKUNG Es wird auf DSGVO Artikel 5, Abschnitt 2 verwiesen.

6.2.2 Die Produkt- und/oder Dienstdokumentation muss angemessene Informationen über die Erfüllung der Anforderungen aus dem gesamten Abschnitt 6 enthalten und darüber, durch welche Funktion, Einstellung oder Maßnahmen dies erreicht wird.

Diese Anforderung gilt für jede Produkt- und Dienstschicht.

6.3 Genauigkeit

6.3.1 Maßnahmenziel:

Den für die Datenverarbeitung Verantwortlichen und den Auftragsverarbeiter in die Lage zu versetzen, Datensätze zu aktualisieren und zu ergänzen.

ANMERKUNG Es wird auf DSGVO Artikel 5, Abschnitt 2, Artikel 16 und Artikel 19 verwiesen.

6.3.2 Das Produkt muss sicherstellen, dass jeder Datensatz, der zur Aufbewahrung personenbezogener Daten bestimmt ist, entweder durch Aktualisierung oder Ergänzung geändert werden kann.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Speicherschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Cloud-Dienstschicht;
- Inhaltsdienstschicht und
- ausgegliederte Geschäftsprozessschicht.

ANMERKUNG Dazu gehört die Vermeidung unveränderlicher Einstellungen ebenso wie die Verwendung von WORM-Medien (WORM, en: write once read many).

6.3.3 Der Dienst muss sicherstellen, dass eine geeignete Funktion bereitgestellt wird, die es autorisierten Benutzern ermöglicht, den Satz der erhobenen und/oder verarbeiteten personenbezogenen Daten zu aktualisieren oder zu ergänzen.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Inhaltsdienstschicht und
- ausgegliederte Geschäftsprozessschicht.

6.3.4 Das Produkt und/oder der Dienst müssen jede Aktualisierungstätigkeit der personenbezogenen Daten mit Zeitstempel, Benutzerkontoname und dem betreffenden Datensatz protokollieren.

Diese Anforderung gilt für die folgenden Produktschichten:

- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Dienstmanagementschicht;
- Selbstbedienungsschicht;
- Cloud-Dienstschicht;
- Inhaltsdienstschicht und
- ausgegliederte Geschäftsprozessschicht.

6.4 Entpersonalisierung von Daten

6.4.1 Maßnahmenziel:

Bereitstellung von Fähigkeiten für die Entpersonalisierung von Daten.

ANMERKUNG Es wird auf DSGVO Artikel 11, Artikel 25 Abschnitt 1, Artikel 32 Abschnitt 1 und Artikel 89 Abschnitt 1 verwiesen.

6.4.2 Das Produkt und/oder der Dienst müssen Maßnahmen vorsehen, um Dateneinträge gegebenenfalls in Pseudonyme umzuwandeln.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemsicht;
- Benutzungsschnittstellenschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Inhaltsdienstschicht,
- ausgegliederte Geschäftsprozessschicht und
- SaaS-Schicht.

6.4.3 Das Produkt und/oder der Dienst müssen Funktionen für die Aggregation erhobener Datensätze in einem Ausmaß bereitstellen, das es unangemessen erscheinen lässt, gegebenenfalls hinter den aggregierten Daten dedizierte betroffene Personen zu identifizieren.

Diese Anforderung gilt für die folgenden Produktschichten:

- Speicherschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Inhaltsschicht und
- ausgegliederte Geschäftsprozessschicht.

6.4.4 Wenn es nicht notwendig ist, die betroffene Person für den angenommenen Zweck der Verarbeitung zu identifizieren, müssen das Produkt und/oder der Dienst entweder durch strenge Funktionalität oder durch Standardeinstellung den Rohdatensatz unmittelbar nach der Aggregation oder Umwandlung in Pseudonyme entsorgen.

Diese Anforderung gilt für die folgenden Produktschichten:

- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgende Dienstsicht:

- ausgegliederte Geschäftsprozessschicht.

6.5 Datenminimierung

6.5.1 Maßnahmenziel:

Sicherstellung, dass die Erhebung und Verarbeitung angemessen und relevant sind und sich auf das erforderliche Minimum an Daten beschränken.

ANMERKUNG Es wird auf DSGVO Artikel 5, Abschnitt 1, Bild c verwiesen.

6.5.2 Das Produkt und/oder der Dienst dürfen in der Datensatzstruktur nur die Felder bereitstellen, die für die bestimmungsgemäße Verwendung unabdingbar sind.

Diese Anforderung gilt für die folgenden Produktschichten:

- Speicherschicht;
- Benutzungsschnittstellenschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Cloud-Dienstschicht;
- Inhaltsschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstschicht und
- Wartungsdienstschicht.

6.5.3 Das Produkt und/oder der Dienst dürfen keine obligatorischen Eingabefelder für Informationen enthalten, die für die bestimmungsgemäße Verwendung nicht erhoben werden müssen.

Diese Anforderung gilt für die folgenden Produktschichten:

- Benutzungsschnittstellenschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Inhaltsschicht;
- ausgegliederte Geschäftsprozessschicht und
- Ausgabedienstschicht.

6.6 Datenübertragbarkeit

6.6.1 Maßnahmenziel:

Ermöglichung der Trennung und des Exports von Datensätzen.

ANMERKUNG Es wird auf DSGVO Artikel 20 verwiesen.

6.6.2 Das Produkt und/oder der Dienst müssen eine Fähigkeit bieten, in ihrer Umgebung gegebenenfalls alle Datensätze zu erheben, die mit einer bestimmten betroffenen Person verknüpft sind.

Diese Anforderung gilt für die folgenden Produktschichten:

- Komponentenschicht;
- Betriebssystemschicht;
- Speicherschicht;
- integrierte Systemschicht;
- Anwendungsschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Cloud-Dienstschicht und
- ausgegliederte Geschäftsprozessschicht.

6.6.3 Das Produkt und/oder der Dienst müssen Fähigkeiten bieten, die nach 6.6.2 erhobenen Datensätze zu übertragen oder zu exportieren.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Speicherschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Übertragungsdienstschicht;
- Cloud-Dienstschicht und
- ausgegliederte Geschäftsprozessschicht.

6.7 Vertraulichkeit

6.7.1 Maßnahmenziel:

Sicherstellung der Datenminimierung und Vertraulichkeit der erhobenen Daten als Standardeinstellung von Produkt und Dienst.

ANMERKUNG 1 Es wird auf DSGVO Artikel 25, Abschnitt 2 verwiesen.

ANMERKUNG 2 Die Zielsetzung der Datenminimierung wird durch die Anforderungen 6.5.2 und 6.5.3 abgedeckt.

6.7.2 Das Produkt und/oder der Dienst müssen sicherstellen, dass die Standardeinstellungen für die Bereitstellung und das Zurücksetzen auf die Werkseinstellungen so vorgenommen werden, dass der Zugang zu den Inhaltsdaten auf ein einziges Konto beschränkt ist.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Speicherschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht;
- Geschäftsprozessschicht;
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Übertragungsdienstschicht;
- Aktualisierungsdienstschicht;
- Cloud-Dienstschicht;
- Inhaltsschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstschicht;
- Wartungsdienstschicht und
- SaaS-Schicht.

6.7.3 Das Produkt und/oder der Dienst müssen sicherstellen, dass das Konto aus 6.7.2 gesperrt wird, sobald ein operatives Konto erstellt wird und zum ersten Mal auf das Produkt oder den Dienst zugegriffen hat.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Speicherschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht;
- Geschäftsprozessschicht;
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Übertragungsdienstschicht;
- Aktualisierungsdienstschicht;
- Cloud-Dienstschicht;
- Inhaltsschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstschicht;
- Wartungsdienstschicht und
- SaaS-Schicht.

6.8 Löschung

6.8.1 Maßnahmenziel:

Bereitstellung der Fähigkeit zur Löschung jedes spezifischen Datensatzes.

ANMERKUNG Es wird auf DSGVO Artikel 17 verwiesen.

6.8.2 Das Produkt und/oder der Dienst müssen die Fähigkeit bieten, den Inhalt eines bestimmten Datenfeldes in einer Tabelle zu löschen, ohne die Integrität der Datentabelle zu verlieren.

Diese Anforderung gilt für die folgenden Produktschichten:

- Komponentenschicht;
- Geräteschicht;
- Betriebssystemschicht;
- Speicherschicht;
- integrierte Systemschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Cloud-Dienstschicht;
- ausgegliederte Geschäftsprozessschicht.

6.9 Fairness

6.9.1 Bestimmung des Benutzeralters

6.9.1.1 Maßnahmenziel:

Bereitstellung von Fähigkeiten zur Bestimmung des Benutzeralters vor der Erhebung.

ANMERKUNG Es wird auf DSGVO Artikel 6, Abschnitt 1, Bild f und Artikel 8 verwiesen.

6.9.1.2 Wann immer der angenommene Zweck der Verarbeitung oder Übertragung die Einwilligung der betroffenen Person erfordert, müssen das Produkt und/oder der Dienst geeignete Maßnahmen vorsehen, um festzustellen, ob es sich bei der betroffenen Person um ein Kind handelt.

Diese Anforderung gilt für die folgenden Produktschichten:

- Benutzungsschnittschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Cloud-Dienstschicht und
- ausgegliederte Geschäftsprozessschicht.

6.9.1.3 Wenn das Produkt und/oder der Dienst feststellen, dass es sich bei der betroffenen Person um ein Kind mit einem Alter unter einem bestimmten Schwellenwert handelt, müssen das Produkt und/oder der Dienst von der Einholung der Einwilligung absehen und der betroffenen Person den Dienst verweigern.

Diese Anforderung gilt für die folgenden Produktschichten:

- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Inhaltsschicht und
- ausgegliederte Geschäftsprozessschicht.

6.9.2 Konfigurierbare Altersgrenze für Kinder

6.9.2.1 Maßnahmenziel:

Die Schwellenwerte für das Alter von Kindern sollen konfigurierbar bleiben.

ANMERKUNG Es wird auf DSGVO Artikel 8, Abschnitt 1 verwiesen.

6.9.2.2 Das Produkt und/oder der Dienst, das/der eine Einwilligung wie bei 6.9.1.2 erfordert, muss den Schwellenwert für das Alter von Kindern je nach Gebiet der Produktnutzung oder des Dienstangebots konfigurierbar halten.

Diese Anforderung gilt für die folgenden Produktschichten:

- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Inhaltsschicht und
- ausgegliederte Geschäftsprozessschicht.

Es wird darauf hingewiesen, dass jeder Mitgliedstaat der EU eine andere Schwelle für das erforderliche Alter der Kinder im Zusammenhang mit der Einwilligung festlegen darf.

6.10 Informationssicherheit

6.10.1 Unbefugte oder unrechtmäßige Verarbeitung

6.10.1.1 Maßnahmenziel:

Zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung.

ANMERKUNG Es wird auf DSGVO Artikel 5, Abschnitt 1, Bild f verwiesen.

6.10.1.2 Das Produkt und/oder der Dienst müssen einen Mechanismus für eine sichere Benutzer-authentifizierung bieten.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht;
- Geschäftsprozessschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Dienstmanagementschicht;
- Selbstbedienungsschicht;
- Cloud-Dienstsicht;
- Inhaltsschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstsicht und
- SaaS-Schicht.

6.10.1.3 Das Produkt und/oder der Dienst müssen durch datenschutzfreundliche Voreinstellungen eine starke Verschlüsselung für Daten während der Übertragung bieten.

Diese Anforderung gilt für die folgenden Produktsichten:

- Betriebssystemschicht;
- Kommunikationsschicht;
- Speicherschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht;
- Geschäftsprozessschicht;
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Selbstbedienungsschicht;
- Integrationsdienstsicht;
- Übertragungsdienstsicht;
- Aktualisierungsdienstsicht;
- Cloud-Dienstsicht;
- Inhaltsschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstsicht;
- SaaS-Schicht und
- Medienwiederherstellungsdienstsicht.

ANMERKUNG Eine Verschlüsselung ist so lange stark, wie die relevante Wissenschaft keine Kenntnis von einer erfolgreich nachgewiesenen Datenschutzverletzung hat.

6.10.1.4 Das Produkt und/oder der Dienst müssen die Fähigkeiten für eine starke Verschlüsselung der gespeicherten Daten bieten.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Speicherschicht;
- Anwendungsschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Dienstmanagementschicht;
- Selbstbedienungsschicht;
- Cloud-Dienstschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstschicht;
- Wartungsdienstschicht;
- SaaS-Schicht und
- Medienwiederherstellungsdienstschicht.

6.10.1.5 Das Produkt und/oder der Dienst müssen die bilaterale Identifizierung von Übertragungspartnersystemen unterstützen.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Kommunikationsschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht;
- Geschäftsprozessschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Dienstmanagementschicht;
- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Übertragungsdienstschicht;
- Aktualisierungsdienstschicht;
- Cloud-Dienstschicht;
- Inhaltsschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstschicht;
- Wartungsdienstschicht und
- SaaS-Schicht.

6.10.2 Datenverlust

6.10.2.1 Maßnahmenziel:

Zum Schutz vor versehentlichem Verlust, Vernichtung oder Beschädigung.

ANMERKUNG Es wird auf DSGVO Artikel 5, Abschnitt 1, Bild f verwiesen.

6.10.2.2 Das Produkt und/oder der Dienst müssen Empfehlungen geben, wie die Datensicherung durchgeführt werden sollte.

Diese Anforderung gilt für die folgenden Produktsichten:

- Betriebssystemschicht;
- Speicherschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht;
- Geschäftsprozessschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Aktualisierungsdienstschicht;
- Cloud-Dienstschicht und
- ausgegliederte Geschäftsprozessschicht.

ANMERKUNG Neben Datensätzen, Dateien und Tabellen sollen hier auch die Tabellenstrukturen betrachtet werden.

6.10.3 Ziele des Informationsschutzes

6.10.3.1 Maßnahmenziel:

Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten.

ANMERKUNG Es wird auf DSGVO Artikel 32, Abschnitt 1, Bild b verwiesen.

6.10.3.2 Das Produkt und/oder der Dienst müssen angemessene Zugriffsebenen bieten, die durch Rollen und konfigurierbare Zugriffsrechte dargestellt werden.

Diese Anforderung gilt für die folgenden Produktsichten:

- Betriebssystemsicht;
- Speichersicht;
- Benutzungsschnittstellensicht;
- integrierte Systemsicht;
- Anwendungssicht;
- Geschäftsprozessschicht und
- Systemmanagementsicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Selbstbedienungssicht;
- Integrationsdienstschicht;
- Übertragungsdienstschicht;
- Aktualisierungsdienstschicht;
- Cloud-Dienstschicht;
- Inhaltsdienstschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstschicht;
- Wartungsdienstschicht und
- SaaS-Sicht.

6.10.3.3 Das Produkt muss jede Verletzung der Datenintegrität an das Systemprotokoll melden.

Diese Anforderung gilt für alle Produktschichten.

6.10.4 Wiederherstellung

6.10.4.1 Maßnahmenziel:

Bereitstellung der Fähigkeiten für eine Wiederherstellung.

ANMERKUNG Es wird auf DSGVO Artikel 32, Abschnitt 1, Bild c verwiesen.

6.10.4.2 Das Produkt und/oder der Dienst müssen die Funktionalität für eine Datenwiederherstellung aus einer Sicherung bieten.

Diese Anforderung gilt für die folgenden Produktschichten:

- Betriebssystemschicht;
- Speicherschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht;
- Geschäftsprozessschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Integrationsdienstschicht;
- Cloud-Dienstschicht und
- ausgegliederte Geschäftsprozessschicht.

6.11 Rechtmäßigkeit

6.11.1 Datenoffenlegung

6.11.1.1 Maßnahmenziel:

Nur personenbezogene Daten zur Verfügung zu stellen, die für einen bestimmten und rechtmäßigen Zweck erhoben werden und für die auch die Übermittlung legitimiert ist.

ANMERKUNG Es wird auf DSGVO Artikel 5 und Artikel 6 verwiesen.

6.11.1.2 Der Dienst muss hinreichend nachweisen, dass die mit dem Dienst bereitgestellten personenbezogenen Daten für einen bestimmten und legitimen Zweck erhoben wurden und dass die Übermittlung dieser personenbezogenen Daten ebenfalls legitimiert ist.

Diese Anforderung gilt für alle Dienstschichten.

6.11.2 Einwilligung

6.11.2.1 Maßnahmenziel:

Die Aufzeichnung der Einwilligung der betroffenen Person und den Widerruf der Einwilligung zu ermöglichen.

ANMERKUNG Es wird auf DSGVO Artikel 6, Abschnitt 1, Bild A, Artikel 7, Artikel 8 und Artikel 49 Abschnitt 1 Bild a verwiesen.

6.11.2.2 Das Produkt und/oder der Dienst müssen jede Anwendungshandlung der betroffenen Person als Benutzer aufzeichnen, die ihre Einwilligung oder den Widerruf der Einwilligung zum Ausdruck bringt, zusammen mit der Art der Handlung, einem Zeitstempel und einem Link zu den Bedingungen, unter denen die Einwilligung erteilt wurde.

Diese Anforderung gilt für die folgenden Produktschichten:

- Benutzungsschnittstellenschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Cloud-Dienstschicht;
- Inhaltsschicht und
- ausgegliederte Geschäftsprozessschicht.

6.12 Widerspruch gegen die Verarbeitung

6.12.1 Maßnahmenziel:

Bereitstellung von Fähigkeiten für die betroffenen Personen, ihr Widerspruchsrecht mit automatisierten Mitteln auszuüben.

ANMERKUNG Es wird auf DSGVO Artikel 21, Abschnitt 5 verwiesen.

6.12.2 Das Produkt und/oder der Dienst müssen die Datenschutzeinstellungen respektieren, die der Benutzer auf seinem Browser-Client vorgenommen hat.

Diese Anforderung gilt für die folgenden Produktschichten:

- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Inhaltsschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstschicht und
- Wartungsdienstschicht.

6.13 Automatisierte Entscheidungsfindung

6.13.1 Maßnahmenziel:

Sicherstellung, dass eine betroffene Person nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung im Einzelfall unterworfen wird.

ANMERKUNG Es wird auf DSGVO Artikel 22, Abschnitt 1 verwiesen.

6.13.2 Das Produkt und/oder der Prozess müssen einen Haltepunkt setzen, der ein menschliches Eingreifen in jeden Prozess erfordert, der die informationsbasierte Entscheidungsfindung unterstützt.

Diese Anforderung gilt für die folgenden Produktschichten:

- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Integrationsdienstschicht und
- ausgegliederte Geschäftsprozessschicht.

6.14 Einschränkung der Verarbeitung

6.14.1 Maßnahmenziel:

Bereitstellung der Fähigkeiten, die Verarbeitung personenbezogener Daten einzuschränken.

ANMERKUNG Es wird auf DSGVO Artikel 18 verwiesen.

6.14.2 Das Produkt und/oder der Dienst müssen Maßnahmen zur Kennzeichnung eines bestimmten Datensatzes und/oder eines Datentabelleneintrags vorsehen und sicherstellen, dass die gekennzeichneten Daten im Rahmen der Verarbeitung nicht für den beabsichtigten Zweck verwendet werden, solange die Kennzeichnung gesetzt ist.

Diese Anforderung gilt für die folgenden Produktschichten:

- Speicherschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht;
- Geschäftsprozessschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Übertragungsdienstschicht;
- Aktualisierungsdienstschicht;
- Cloud-Dienstschicht;
- ausgegliederte Geschäftsprozessschicht und
- Ausgabedienstschicht.

ANMERKUNG Die Verarbeitung zur Beachtung der Kennzeichnungen und die Bereitstellung von Beweismitteln in einem Gerichtsverfahren sind erlaubt.

6.14.3 Das Produkt und/oder der Dienst müssen das Setzen und den Widerruf der Kennzeichnung mindestens mit Benutzernamen und Zeitstempel in einem Protokolleintrag aufzeichnen.

Diese Anforderung gilt für die folgenden Produktschichten:

- Speicherschicht;
- Benutzungsschnittstellenschicht;
- integrierte Systemschicht,
- Anwendungsschicht,
- Geschäftsprozessschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Selbstbedienungsschicht;
- Cloud-Dienstschicht;
- ausgegliederte Geschäftsprozessschicht.

6.15 Speicherbegrenzung

6.15.1 Maßnahmenziel:

Die Identifizierung der betroffenen Personen nicht länger zu ermöglichen, als es für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist.

ANMERKUNG 1 Es wird auf DSGVO Artikel 5, Abschnitt 1, Bild e verwiesen.

ANMERKUNG 2 Es wird auf 6.4 verwiesen.

6.15.2 Das Produkt und/oder der Dienst müssen Fähigkeiten bieten, bestimmte Datensätze oder Datentabelleneinträge in Verbindung mit einem zeitstempelbezogenen Schwellenwert am Ende der rechtmäßigen Aufbewahrungsfrist zu löschen.

Diese Anforderung gilt für die folgenden Produktschichten:

- Anwendungsschicht;
- Geschäftsprozessschicht und
- Systemmanagementschicht.

Diese Anforderung gilt für die folgenden Dienstschichten:

- Dienstmanagementschicht;
- Selbstbedienungsschicht;
- Integrationsdienstschicht;
- Cloud-Dienstschicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedienstschicht.

6.16 Transparenz

6.16.1 Informationen

6.16.1.1 Maßnahmenziel:

Bereitstellung der Fähigkeiten, die betroffene Person in allen Aspekten, die mit ihrer Einwilligung zusammenhängen, zu informieren.

ANMERKUNG Es wird auf DSGVO Artikel 7 und Artikel 13 verwiesen.

6.16.1.2 Das Produkt und/oder der Dienst müssen einen Dialogpunkt enthalten, der für die Verwendung durch die Datenschutzerklärung und weitere Informationen zur Einwilligung vorgesehen ist.

Diese Anforderung gilt für die folgenden Produktschichten:

- Benutzungsschnittstellenschicht;
- integrierte Systemschicht;
- Anwendungsschicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Selbstbedienungssicht;
- Integrationsdientsicht;
- Übertragungsdientsicht;
- Aktualisierungsdientsicht;
- Cloud-Dientsicht;
- Inhaltsdientsicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedientsicht;
- Wartungsdientsicht.

6.16.1.3 Das Produkt und/oder der Dienst müssen einen Dialogpunkt enthalten, der die Adresse und Kontaktinformationen des für die Datenverarbeitung Verantwortlichen enthalten soll.

Diese Anforderung gilt für die folgenden Produktsichten:

- Benutzungsschnittstellensicht;
- integrierte Systemsicht;
- Anwendungssicht und
- Geschäftsprozessschicht.

Diese Anforderung gilt für die folgenden Dienstsichten:

- Selbstbedienungssicht;
- Integrationsdientsicht;
- Übertragungsdientsicht;
- Aktualisierungsdientsicht;
- Cloud-Dientsicht;
- Inhaltsdientsicht;
- ausgegliederte Geschäftsprozessschicht;
- Ausgabedientsicht und
- Wartungsdientsicht.